WHAT IS CLAIMED IS:

1. A method for authenticating a mobile node in a wireless local area network including at least two access points for setting up wireless association between the mobile node and an authentication server for authenticating the mobile node, the method comprising the steps of:

(a) when the mobile node associates with a first access point and performs initial authentication, receiving, by the mobile node, a first session key for secure communication from the authentication server by using a first private key generated with a secret previously shared with the authentication server, and receiving, by the first access point, the first session key from the authentication server by using a second private key previously shared with the authentication server; and

(b) when the mobile node is handed over from the first access point to a second access point and performs re-authentication, receiving, by the mobile node, a second session key for secure communication from the authentication server by using a third private key generated with authentication information generated during previous authentication and shared with the authentication server, and receiving, by the second access point, the second session key from the authentication server by using the second private key previously shared with the authentication server.

2. The method of claim 1, wherein step (a) comprises the steps of:

generating the first private key with the secret previously shared by the mobile node and the authentication server;

generating, by the mobile node, first authentication information to be used during next authentication request and transmitting a first enciphered message generated by enciphering the first authentication information with the first private key to the authentication server;

storing, by the authentication server, the first authentication information acquired by deciphering the first enciphered message with the first private key and

generating the first session key for secure communication;

transmitting, by the authentication server, a second enciphered message generated by enciphering the first session key and the first authentication information with the first private key to the mobile node, and transmitting a third enciphered message generated by enciphering the first session key and the first authentication information with the second private key previously shared with the first access point, to the first access point;

acquiring, by the first access point, the first session key by deciphering the third enciphered message with the second private key, and acquiring, by the mobile node, the first session key by deciphering the second enciphered message with the first private key; and

performing secure communication by the mobile node and the first access point by using the first session key.

3. The method of claim 2, wherein the first authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number.

4. The method of claim 3, wherein the first enciphered message includes a permanent identifier of the mobile node and the first authentication information.

5. The method of claim 3, wherein the second enciphered message includes the first session key, a permanent identifier of the mobile node, and the random number.

6. The method of claim 3, wherein the third enciphered message includes the first session key and the random number.

7. The method of claim 1, wherein step (b) comprises the steps of:

generating, by the mobile node and the authentication server, the third private key with the first authentication information generated by the mobile node during

previous authentication;

generating, by the mobile node, second authentication information to be used during next authentication request, and transmitting a fourth enciphered message generated by enciphering the second authentication information with the third private key to the authentication server;

storing, by the authentication server, the second authentication information acquired by deciphering the fourth enciphered message with the third private key and generating the second session key for secure communication;

transmitting, by the authentication server, a fifth enciphered message generated by enciphering the second session key and the authentication information with the third private key to the mobile node, and transmitting a sixth enciphered message generated by enciphering the first session key and the authentication information with the second private key previously shared with the second access point to the second access point;

acquiring, by the second access point, the second session key by deciphering the sixth enciphered message with the second private key, and acquiring, by the mobile node, the second session key by deciphering the fifth enciphered message with the third private key; and

performing secure communication by the mobile node and the second access point by using the second session key.

8. The method of claim 7, wherein the second authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number.

9. The method of claim 8, wherein the fourth enciphered message includes a previous temporary identifier of the mobile node and the second authentication information.

10. The method of claim 8, wherein the fifth enciphered message includes the second session key and the random number.

11. The method of claim 8, wherein the sixth enciphered message includes the second session key, the random number, and the temporary identifier of the mobile node.

12. A method for performing authentication by a mobile node in a wireless local area network including at least two access points for setting up wireless association with the mobile node and an authentication server for authenticating the mobile node, the method comprising the steps of:

when associating with a first access point and performing initial authentication, generating a first private key with a secret previously shared with the authentication server;

generating first authentication information to be used during next authentication request, and transmitting a first enciphered message generated by enciphering the first authentication information with the first private key to the authentication server;

upon receiving a second enciphered message from the authentication server in response to the first enciphered message, acquiring a first session key by deciphering the second enciphered message with the first private key; and

performing secure communication with the first access point by using the first session key.

13. The method of claim 12, wherein the first authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number.

14. The method of claim 13, wherein the first enciphered message includes a permanent identifier of the mobile node and the first authentication information.

15. The method of claim 13, wherein the second enciphered message includes the random number and the first session key.

16. The method of claim 12, further comprising the steps of:

when being handed over from the first access point to a second access point and performing re-authentication, generating a second private key with the first authentication information generated during previous authentication;

generating second authentication information to be used during a next authentication request, and transmitting a third enciphered message generated by enciphering the second authentication information with the second private key to the authentication server;

upon receiving a fourth enciphered message from the authentication server in response to the third enciphered message, acquiring a second session key by deciphering the third enciphered message with the second private key; and

performing secure communication with the second access point by using the second session key.

17. The method of claim 16, wherein the second authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number.

18. The method of claim 17, wherein the third enciphered message includes a previous temporary identifier of the mobile node and the second authentication information.

19. The method of claim 17, wherein the fourth enciphered message includes the random number and the second session key.

20. A method for performing authentication of a mobile node by an authentication server in a wireless local area network including at least two access points for setting up wireless association with the mobile node and an authentication server for authenticating the mobile node, the method comprising the steps of:

when the mobile node associates with a first access point and performs initial authentication, generating a first private key with a secret previously shared with the mobile node;

upon receiving a first enciphered message from the mobile node, acquiring first authentication information to be used during next authentication by deciphering the first enciphered message with the first private key;

generating a first session key for secure communication of the mobile node;

generating a second enciphered message by enciphering the first session key and the first authentication information with the first private key, and transmitting the second enciphered message to the mobile node; and

generating a third enciphered message by enciphering the first session key and the first authentication information with a second private key previously shared with the first access point, and transmitting the third enciphered message to the first access point.

21. The method of claim 20, wherein the first authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number.

22. The method of claim 21, wherein the first enciphered message includes a permanent identifier of the mobile node and the first authentication information.

23. The method of claim 21, wherein the second enciphered message includes the random number and the first session key.

24. The method of claim 21, wherein the third enciphered message includes the first session key and the random number.

25. The method of claim 20, further comprising the steps of:

when the mobile node is handed over from the first access point to a second access point and performs re-authentication, generating a third private key with the first authentication information received from the mobile node during previous authentication;

upon receiving a fourth enciphered message from the mobile node, acquiring second authentication information to be used during next authentication by deciphering

the fourth enciphered message with the third private key;

generating a second session key for secure communication of the mobile node;

generating a fifth enciphered message by enciphering the second session key and the second authentication information with the third private key and transmitting the fifth enciphered message to the mobile node; and

generating a sixth enciphered message by enciphering the second session key and the second authentication information with the second private key previously shared with the second access point, and transmitting the sixth enciphered message to the second access point.

26. The method of claim 25, wherein the second authentication information includes a temporary identifier of the mobile node, a password for generating a private key to be used during next authentication, and a random number.

27. The method of claim 26, wherein the fourth enciphered message includes a permanent identifier of the mobile node and the second authentication information.

28. The method of claim 26, wherein the fifth enciphered message includes the random number and the second session key.

29. The method of claim 26, wherein the sixth enciphered message includes the second session key and the random number.

30. A method of performing authentication of a mobile node by an access point with which the mobile node initially associates or re-associates due to handover, in a wireless local area network including the access point for setting up association with the mobile node and an authentication server for authenticating the mobile node, the method comprising the steps of:

when associating with the mobile node and performing authentication, receiving an enciphered message from the authentication server;

acquiring a session key for secure communication with the mobile node by deciphering the enciphered message with a private key previously shared with the authentication server; and

performing secure communication with the mobile node by using the session key.

31. The method of claim 30, wherein the enciphered message includes a temporary identifier generated by the mobile node during previous authentication, and a random number.